(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 January 2005 (27.01.2005)

PCT

(10) International Publication Number
WO 2005/008385 A3

(51) International Patent Classification[7]: G06F 12/14

(21) International Application Number: PCT/US2004/021621

(22) International Filing Date: 7 July 2004 (07.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/614,765 7 July 2003 (07.07.2003) US
60/537,421 16 January 2004 (16.01.2004) US

(71) Applicant *(for all designated States except US)*: **CRYPTOGRAPHY RESEARCH, INC.** [US/US]; 575 Market Street, Suite 2150, San Francisco, CA 94105 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KOCHER, Paul, C.** [US/US]; 134 Fillmore Street, San Francisco, CA 94117 (US). **JAFFE, Joshua, M.** [US/US]; 1833 Church Street, San Francisco, CA 94131 (US). **JUN, Benjamin, C.** [US/US]; 133 Duncan Street, San Francisco, CA 94110 (US). **LAREN, Carter, C.** [US/US]; 86 Barcelona Avenue, San Francisco, CA 94115 (US). **PEARSON, Peter, K.** [US/US]; 5624 Victoria Lane, Livermore, CA 94550 (US).

(74) Agent: **RADLO, Edward, J.**; Sonnenschein, Nath & Rosenthal, Post Office Box 61080, Wacker Drive Station, Sears Tower, Chicago, IL 60606 (US).

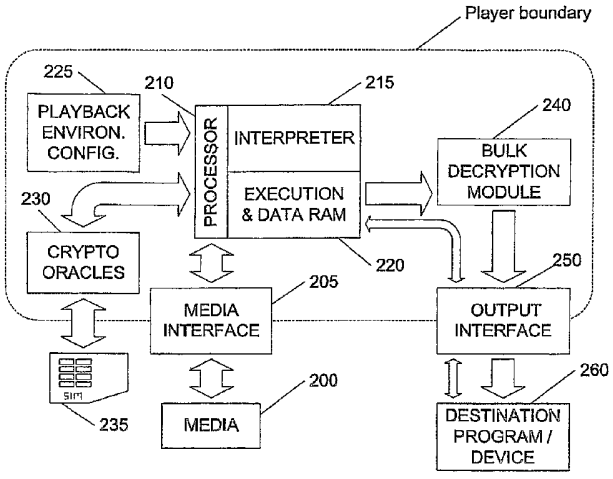
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: REPROGRAMMABLE SECURITY FOR CONTROLLING PIRACY AND ENABLING INTERACTIVE CONTENT



(57) Abstract: Technologies are disclosed to transfer responsibility and control over security from player makers to content authors by enabling integration of security logic and content. An exemplary optical disk (200) carries an encrypted digital video title combined with data processing operations (225) that implement the titles security policies and decryption processes. Player devices include a processing environment (e.g., a real-time virtual machine), which plays content by interpreting its processing operations. Players also provide procedure calls to enable content code to load data from media, perform network communications, determine playback environment configurations (225), access secure non-volatile storage, submit data to CODECs for output (250), and/or perform cryptographic operations. Content can insert forensic watermarks in decoded output for tracing pirate copies. If pirates compromise a player or title, future content can be mastered with security features that, for example, block the attack, revoke pirated media, or use native code to correct player vulnerabilities.

WO 2005/008385 A3

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
19 May 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/21621

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 12/14

US CL : 713/185

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/201,232,233; 705/51,56,57; 713/2,170,171,181,185,190; 369/26.01,30.01,47.12,47.15; 711/108, 365/49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,314,409 B2 (SCHNECK et al) 6 November 2001, fig. 11: Table 1, fig. 12: item S1212 , col. 7, lines 41-48, col. 15 lines 30-40, col. 19 lines 61-67, col. 20 lines 1-4, 30-35, col. 31 lines 20-25.	1-4, 11
A	US 5,191,611 A (LANG) 2 March 1993, Entire Document.	1-4, 11
A	US 5,638,443 A (STEFIK et al) 10 June 1997, Entire Document.	1-4, 11
A	US 5,392,351 A (HASBE et al) 21 February 1995, Entire Document.	1-4, 11
A	US 5,450,489 A (OSTROVER et al) 12 September 1995, Entire Document.	1-4, 11

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 November 2004 (26.11.2004)	15 APR 2005
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer for Michelle L. Eason Andrew Caldwell Telephone No. 305-3900

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/21621

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/21621

BOX III. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group1, claim(s) 1-4 and 11, drawn to a method for limiting access to non-volatile digital storage contained in a device executing instructions in a Touring-complete interpreter.

Group 2, claim(s) 5-7, drawn to a digital optical storage medium containing encrypted audiovisual content playback on any of a plurality of device architectures.

Group 3, claim(s) 8-10, drawn to an automated method for enabling a playback device containing a nonvolatile memory to determine whether permission to use digital optical disk media has been revoked.

The inventions listed as Groups 1-3 do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: Group 1 includes limitations directed towards access control via authentication of a hash value of executable instructions, Group 2 is directed towards an optical disk with a playback program encoded thereupon which when executed determines which of a plurality of security weaknesses are present in a playback (executing) device, Group 3 is directed towards limiting access to a digital storage medium via determining if an instance of permission to utilize the medium has been revoked based upon reading an identifier from the medium and comparison with a revocation list.

No generic linking claim(s) is found in the claim groups.

The 3 claim groups are independent and distinct from one another as per MPEP Sec. 802.21 and within the meaning of 35 USC 121.

The requirement for unity of invention referred to in Rule 13.1 is not met. There is no technical relationship among the 3 inventions claimed in claim groups 1-3 involving one or more of the same or corresponding technical features.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/21621

Continuation of B. FIELDS SEARCHED Item 3:
EAST
NPL